

Potpourri Topics from recent issues of the Ask Woody Newsletter

(a weekly email newsletter about Windows computers
and software, and related issues, from askwoody.com)

Compiled by Gary Patrick
Lexington Computer & Technology Group

4/22/2020

Table of Contents

Topic 1) The “Ask Woody” Newsletter has resumed a free edition:

Once a week, a subset of the Ask Woody Plus paid newsletter:

- likely three articles a week out of four-to-six in the Plus edition.

- a sample copy is at:

<https://www.askwoody.com/askwoody-newsletter-alerts/welcome-to-the-askwoody-free-newsletter/>

This issue has an article “Is a Chromebook right for you,” within the objectives of the newsletter to provide user help for Windows 7, 8, and operating systems alternatives to Windows 7 and 8, as well as the primary coverage of Windows 10 and applications.

A link to sign up for the free edition is

<https://cdn.forms-content.sg-form.com/fadcab1b-6abe-11ea-9648-2a7e788be8da>

A bonus is free access to the “Forums” section of Readers’ comments and blogs - examples are: 1) “Setting up a Standard User Account in Windows 10,” and 2) Reader Discussion about Backup Imaging Software.

Go to slide #29 for web links. One can search the Forums by any keyword(s).

Topic 2) Is your cloud-stored data there forever? (beginning with slide #3)

Including a survey of Encryption Software

(But there is an unanswered question whether adding encryption now can really overwrite and hide data already stored earlier in the Cloud unencrypted - very likely not).

Topic 3) Updates to the Ask Woody Ultimate Utilities List (beginning in slide #21)

When you delete data stored in your “Cloud” account - - is your deleted data really gone?

(by Fred Langa, Ask Woody Plus Newsletter, Issue 17.10.0, March 9, 2020.)

Most Windows users know that clicking "delete" does not actually erase local files; it merely modifies an index table.

The same holds true for your data stored in the cloud.

- Those files can remain in remote backups or in online services' logs for a very long time.
- There's no way you, the end user, can guarantee deletion/erasure of anything you post online or save in the cloud.
- Even deleting your entire online/cloud account won't necessarily delete your files.
- Your previous files and data will almost surely live on in your ISP's or cloud provider's backups and logs — at least for a while.

If your files are on someone else's server -

- only they control the for-real data retention/deletion rules.
- the retention period might be weeks or months, especially if the service has a "previous versions" or "recover your accidentally deleted account" feature.
- (Obviously, if you can recover deleted data, there must be backups somewhere.)
- these backups should eventually age out and get overwritten, but there's no way for users to know how long that will take.

In some cases, the data might be retained literally for years — for example, in jurisdictions where ISPs and/or cloud-service providers believe they need to hang on to old user data should there be future legal actions.

Fortunately, an easy way exists to keep your left-online data protected, even when it's no longer under your full control. How? Use encryption!

If you encrypt your files BEFORE you upload them, it won't matter at all where they end up or who might have access to them. Only you know the de-encryption key.

With quality encryption (say, AES-256 or better) and a strong password,

- the contents of your online/cloud-based files will be completely secure.
- Let your files sit on the cloud-based server forever — who cares?
- No one will be able to read them! (Except the U.S. National Security Agency)

File encryption is easy; there are many tools available.

Some cloud-service providers offer their own built-in encryption -
two examples:

- Microsoft's OneDrive offers a "Personal Vault" (new in October 2019) applies BitLocker encryption to selected cloud-based OneDrive files:

User Guide: by Seth Patton, General Manager, Microsoft 365 products:
https://www.microsoft.com/en-us/microsoft-365/blog/2019/06/25/onedrive-personal-vault-added-security-onedrive-additional-storage/?mc_cid=6d84eac8a7&mc_eid=c3d7529d95

- Some applications, such as the MS Office suite, offer good built-in encryption (i.e., "password protection") for files, although you must enable it on a file-by-file basis.

For example, within Word, click "File" → "Info," → "Protect Document,"
→ "Encrypt with Password."

(see Figure 1, next slide).

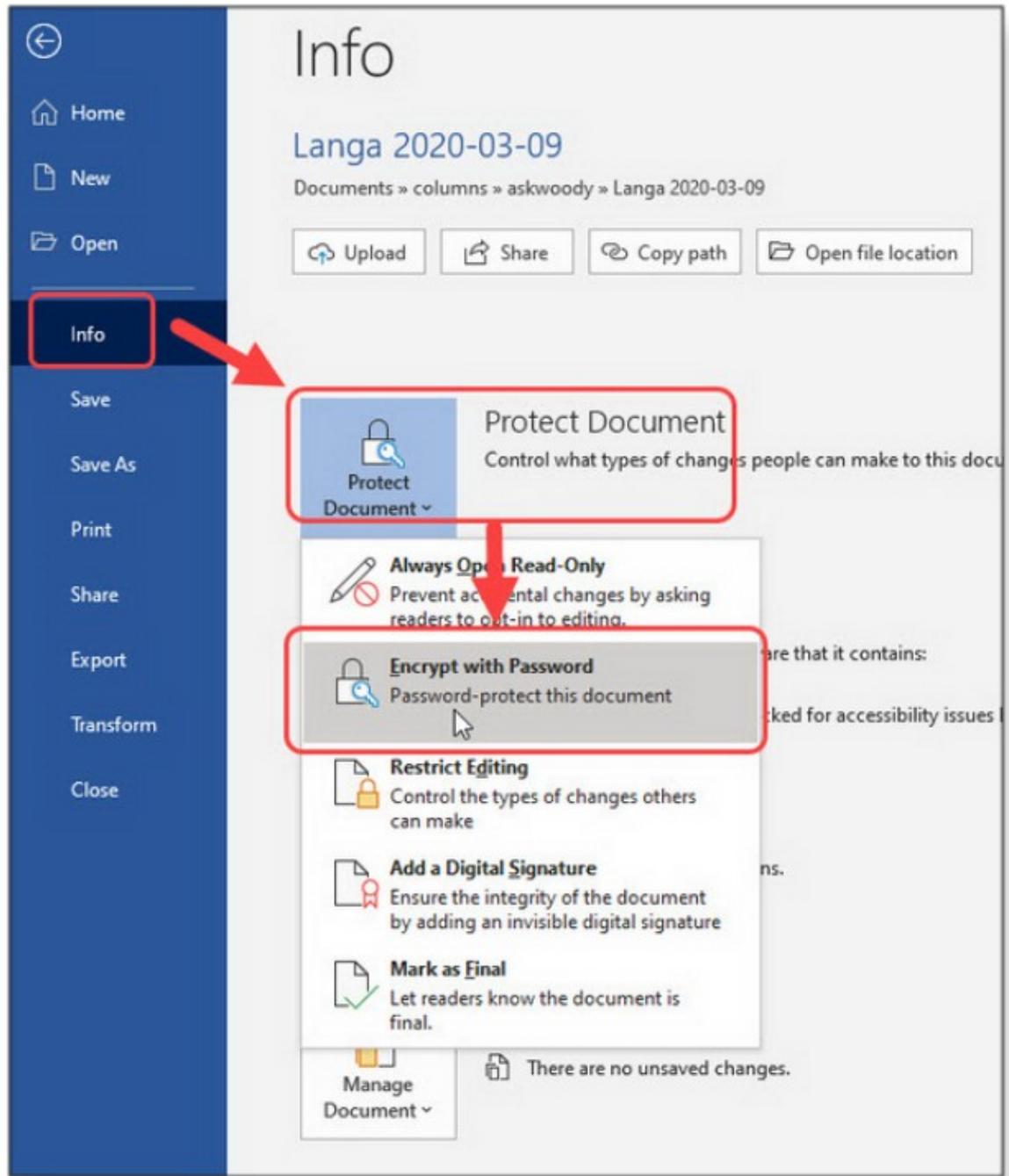


Figure 1. MS Office apps have file encryption built in. (Shown: The current Office 365/Word)

But cloud-based and built-in encryption options

- still force you to trust the skills and policies of the provider.
- The encryption isn't truly under your control. Remedy –

Use a third-party encryption app to scramble files before uploading.

When the encryption and decryption happen locally, on your PC, the remote-cloud provider never sees your password or the unencrypted contents of your files. You'll know that only you hold the keys!

Examples of 3rd-party software:

1) 7-Zip (free/open source). It's not tied to any one app, file type, or service.

- it can encrypt literally any file or folder on your machine.
- as a bonus, it efficiently compresses the contents to save space.

Fred gives this Google search to locate other encryption software:

https://www.google.com/search?q=file+encryption+windows&mc_cid=6d84eac8a7&mc_eid=c3d7529d95

The results of this Google search list include two articles that are reviews by PCMag and TechRadar: (links on the next slide)

The Best Encryption Software for 2020, by Neil J. Rubenking, PCMag, Updated March 24, 2020. Full reviews of each selection available <https://www.pcmag.com/picks/the-best-encryption-software>

Best Encryption Software of 2020, by Nicholas Fearn & Brian Turner, TechRadar.com, January 29, 2020; Three-four paragraphs about each. <https://www.techradar.com/best/best-encryption-software>

PCMag's Choices:

- FolderLock
- AxCrypt Premium
- CertainSafe Digital Safety Box
- NordSafe
- Intercrypto Advanced Encryption Package

TechRadar's Choices:

- AxCrypt
- Folder Lock
- CryptoExpert
- CertainSafe
- VeraCrypt

Neither of these articles covers Boxcryptor, that has been added to the Ask Woody selected Ultimate Utilities List. But there's a very complete review of it by Jacob Roach, Deputy Editor, Cloudwards (Last Updated: 10 Mar 2020) <https://cloudwards.net/boxcryptor-review/>:

Boxcryptor is a popular, free encryption application that allows you to sync your encrypted files easily with more than 30 cloud storage, EFSS and online backup providers.

- Boxcryptor is mostly focused on cloud storage, but it can also encrypt local files.
- It works from within Windows File Explorer as well as within its own application window.
- Boxcryptor actually mounts a virtual drive, so your files and folders will show up as a hard drive alongside your others.
- Additionally, Boxcryptor will automatically detect and file any cloud storage folders you have on your machine
- Boxcryptor supports on-the-fly encryption. Instead of encrypting an entire folder, each file within the folder is encrypted separately. That allows you to easily decrypt a single file and edit it without having to decrypt, and thus reencrypt, the entire folder.

Boxcryptor (continued)

Strengths:

- Easy to use
- provides its full protection for as many files as you want.
- Portable app available – plug it into any Windows, iOS or Linux p.c.
- Works with iOS and Android, providing the full functionality of the desktop application.
- Sharing with non-Boxcryptor users
- RSA key management; zero knowledge password for tight security
- Extensive user guides

Weaknesses, for the free plan:

- You can use your account on only two devices and can sync with
- only one cloud storage provider
- Help limited to Community Forum; direct help support only for paying users
- The paid version has strange pricing restrictions and no refunds.

(With a paid premium plan, you can add as many locations as you want, allowing you to encrypt network-attached storage, USB drives, entire disks, WebDAV locations and more).

– – – –

Back to the selections of Encryption Programs by PC Mag and TechRadar – see next slides:

Folder Lock: PCMag Editors' #1 Choice, score 4.5 of 5;
2nd choice by TechRepublic.

Folder Lock can lock access to files for quick, easy protection, and also keep them in encrypted lockers for serious protection. It combines a wide range of features with a bright, easy-to-use interface.

There is a free version, but the pro version is available for a one-time fee of \$39.95 which opens up more advanced and useful security features:

Pros: Encrypted lockers protect files and folders.

- Secure online backup.

- Can lock files and folders, making them invisible.

- File shredding.

- Free space shredding.

- Self-decrypting files.

- Many useful bonus features: you can set a decoy password, hacker deterrents, log unauthorised login attempts, back up all your passwords and get notified on potential brute-force attacks. (TechRadar)

Cons: Mainly mobile oriented (TechRadar: protect your personal files, photos, videos, contacts, wallet cards, notes and audio recordings stored in your handset).

- Product serial number stands in for master password by default.

- Locked files are not encrypted.

- Secure backup requires separate subscription.

AxCrypt Premium: PCMag Editors' Choice, score 4.5 of 5; 1st by TR
Makes encryption simple enough for any user, and even offers public key cryptography for secure sharing of encrypted files. \$42/year (TechRadar)
There is a free version but it's very limited; best considered as a get-familiar trial.

Pros:

- Very easy to use.
- Will automatically protect files saved on services such as Google Drive and Dropbox. (TechRadar)
- Strong encryption (128-bit or 256-bit AES encryption) (TechRadar)
- Handles editing encrypted files.
- Secure sharing using public key cryptography.
- Secure file deletion.
- Generates memorable passwords.
- Secure online password storage.

Cons:

- Can be risky if you don't ensure local security of your PC.
- Mainly mobile-device oriented (TechRadar)

CertainSafe Digital Safety Deposit Box: PCMag Ed. Choice, score 4.5.
4th choice by TechRadar.

30-day free trial available, after which a subscription costs \$144 per year for 100GB and up to 100 free guests.

Pros:

- Can store and share documents, private messages, photos, videos and other files without exposing them to third-party sources.
- You can collaborate and communicate with colleagues through the system, with all correspondence encrypted.
- When storing your sensitive files in the cloud, CertainSafe makes security its top priority, without sacrificing ease of use.
- Renders bulk data breach of cloud-stored files impossible.
- Authenticates user to server and vice versa.
- Retains past file versions.
- Secure chat.

Cons:

- Relatively expensive.
- Not everyone wants cloud-based security.
- If you forget password or security answers, you lose all access.
- Office integration currently unavailable.

NordLocker encryption tool, From the makers of the popular NordVPN, is very easy to use, but still lacks a few important features. PCMag 3.5

Pros:

- Very easy to use.
- Users can securely share encrypted files.
- Capacity-limited free edition available.
- Integrates with Dropbox for sharing.

Cons:

- No secure deletion of unencrypted original files.
- Lacks a two-factor authentication option.

InterCrypto's Advanced Encryption Package is by far the most feature-rich encryption tool we've tested. But its awkward and dated interface make it one that should be reserved for experts. MSRP \$49.95 PCMag score, 4.0; (not mentioned by TechRadar).

Pros:

- Offers 17 encryption algorithms.
- Supports PKI.
- Secure deletion.
- Password generator.
- Encrypts text to/from the clipboard.
- Command-line operation.

Cons:

- Awkward, dated user interface.
- Password generator doesn't work well.
- Some features described in Help system are absent.

CryptoExpert, rated #3 by TechRadar, (not mentioned by PCMag).
a free 30-day trial available, after which CryptExpert costs \$59.95 to buy.
It is Windows desktop software which offers secure data vaults for all
your data, ensuring it's always protected from potential breaches.

Pros:

- provides more powerful encryption than some of the other tools and apps listed in this article, boasting fast on-the-fly operation.
uses Blowfish, Cast, 3DES and AES-256 encryption algorithms. The latter are highly effective and industry-acclaimed.
- can back up a range of different files, including certificates, Word, Excel and PowerPoint files, multimedia files and email databases.
- can secure vaults of unlimited size,
- works with 32-bit and 64-bit versions of Windows 7, 8 and 10.

Cons:

- It may be too complicated for some
- Available for Windows only

VeraCrypt, #5 by TechRadar, (not mentioned by PCMag); free.

VeraCrypt is one of the most popular security tools, providing you with enterprise-grade encryption for important data.

- It supports Windows, iOS, and Linux devices. (Cloudwards review)
- Free, open-source software
- The system is quite easy to use, and all it really does is add encrypted passwords to your data and partitions. All you have to do is give the tool a few details about your data, such as volume size, location and specified hashing algorithms – and then the program does its thing.
- It has a portable version.
- What's also nifty about VeraCrypt is that it's immune to brute-force attacks, so you never have to worry about hackers decrypting your passwords and other sensitive data.

Here are additional detailed reviews of VeraCrypt:

<https://www.ghacks.net/2018/09/14/veracrypt-encryption-software-review/> and <https://www.cloudwards.net/veracrypt-review/> 2020/04/07.

Veracrypt (continued, from cloudwards.net review):

Strengths:

- Whole-disk encryption
- Operating system encryption
- Multiple algorithm options
- Free
- Open-source
- Hidden volumes & operating systems
- Provision to create a Rescue Disk to repair damaged Boot Loader or Decryption data in the case of encrypted partitions.

Weaknesses:

- Can be difficult to use
- Few support options
- No cloud storage integration
- No sharing options

Other Encryption Software to consider (from TechRadar)

Secure IT 2000 is a file encryption program that also compresses your files. This means that it may take a little longer than some other programs, but it does mean your files are potentially more manageable after. A master password is required to access any files, which can be a little limiting if you'd prefer to have different passwords for different files, not least if you're looking to share some of them with family and/or friends.

Concealer is a file encryption program specifically for Apple Mac computers. Rather than encrypt all files on your harddrive, instead it provides an encrypted area for you to drag files into - which means you need to ensure you delete the original copy so as to avoid having both encrypted and non-encrypted versions on your harddrive. You can also choose your preferred encryption strength as 128 or 256-bit.

Renee File Protector is another piece of file encryption software for Windows, but this one allows you to have different passwords for different files or folders, effectively creating multiple security levels. Alternatively, you can just stick with a master password if required. And if you forget any of your passwords, Renee File Protector can provide prompts to allow you to recover them, which is handy.

SensiGuard doesn't just encrypt your files and folders, it also hides them so that they will remain hidden from unauthorized users, which is a potentially useful feature. Additionally, you can also securely shred files, which means that it's even harder for hackers to locate any sensitive files on your harddrive that you've already encrypted, or deleted.

— — — —

In conclusion, quoting PCMag, good file encryption is really the only way to keep your private files stored online truly private — even when they're no longer in your possession or under your control!

Updates to the Ask Woody Ultimate Utilities List

By T. B. Capen, Ask Woody Newsletter, Issue 17.10.0, March 9, 2020

The following are suggestions from the Ask Woody Newsletter readers:

1) ccPortable (OlderGeeks.com download): “Many long-time Windows users have lamented their loss of trust in the once immensely popular CCleaner. Back in the Windows 7 era, it was the go-to utility for safely scanning and cleaning PCs. But all is not lost: several forum members recommended the free and portable version of CCleaner as a good alternative. It's posted on the OlderGeeks site, so you know it's safe from malware and unwanted add-ons.” [T.B. Capen]

2) Reader “Microfix” suggested BleachBit as yet another portable and free cleaning utility. Its focus is reducing disk clutter and enhancing privacy.

3) Startpage is a substitute for DuckDuckGo Search (listed below).

- touts itself as the most private search engine in the world.
- works as a privacy bridge between your browser and Google Search.
- you won't be tracked,
- but the top results will still contain lots of ads.

4) TreeSize (free) displaced ACDSee in the Top Ten.

”Don't get me wrong: I use the ACDSee photo-editing app every day to put out the newsletter. But TreeSize is one of those highly recommended and indispensable tools for investigating what's using up your file storage space.” [T.B. Capen]

(from here on, the new recommendations are for-pay programs)

5) In turn, ACDSee Photo (paid) displaces Irfanview (free).

”IrfanView is a fine free photo editor. I still have it installed on my PCs. It has a tool for many image-editing tasks. But if you're trying to process large numbers of photos rapidly— especially RAW images from Canon or Nikon cameras — ACDSee is simply a more professional-level product.” [T.B. Capen]

6) Backup Outlook: Michael Austin suggested this backup utility.

This app is targeted at keeping Outlook data and settings safe and easily recoverable. Backup Outlook costs USD \$39.95, but you can try a limited edition for 14 days.

7) Directory Opus by GPSoftware: DennyB submitted this entry as an excellent substitute for Windows' File Explorer. The one catch? It's not cheap. The "Light" version is priced at AUD \$49, or about USD \$33, while the "Pro" edition is AUD \$89 (about USD \$59). You can try it free for up to 60 days.

The Ultimate Utilities List continues on the next slide:

The Top Ten of the Ask Woody Ultimate Utilities: Our list of must-haves -
When we set up a new machine, we install the following apps first:

- Office 365 (subscription; primarily for Word, Excel, OneDrive, OneNote, and Outlook)
- Firefox and Google Chrome) (free)
- Dropbox (reluctantly; free/paid)*
- 7-Zip (free; file compression/encryption)
- VideoLAN VLC media player (free)
- Apple iTunes (free; Winamp used to be a popular alternative)
- Notepad ++ (free/donation; excellent text editor)
- JAM TreeSize Free (free; disk-use viewer, file structure and sizes occupied)
- Oracle VM VirtualBox (free; virtual machines)
- Netflix, Pandora, and Spotify (subscription; because you gotta have some fun)

For browser security, also set DuckDuckGo as your default search engine.

* ed. Note - no indication given why Mr. Capen says “reluctantly” about Dropbox. It may be because one gets only 2 GB of storage in a free account.

The rest of the Ultimate Utilities List continues on Slide #'s 26-28.

A Caution Note about free utilities : a couple of important reminders about installing and using utilities that delve deep into Windows:

- Always be sure you have a full and current system backup before running the app. That's especially true of "system cleaners" and "performance enhancers."
- Next, watch out for those annoying and potentially dangerous software offers that often come with free utilities.
 - The Adobe Acrobat Reader installer, for instance, has included pre-checked offers for Google Chrome and McAfee.
 - The various utilities hosted by our OlderGeeks friends are guaranteed to be free of tagalong software and malware: <https://oldergeeks.com>
- A future Ultimate Utilities article will list apps reviewed in our Freeware Spotlight columns.

The Ask Woody Ultimate Utilities List, continued:

General Utilities:

- Mythicsoft Agent Ransack (free; search)
- Avanquest PowerDesk Pro (paid; file management)
- Copernic (free trial/paid; desktop search)
- DOSBox (free; MS-DOS emulator)
- Nitro Pro (free trial/paid; PDF creator)
- Karen Kenworthy's Replicator (free; a classic Windows backup app)
- TechSmith Snagit (trial/paid; screen capture)
- TeamViewer (free/paid; remote access/control)

Media applications:

- ACDSee Photo (paid; image editing and management)
- GIMP (free; a powerful and classic image editor)
- Mp3tag (free; music metatag editor)
- Paint.NET (free; image editor)

Browsing security:

- CyberGhost (subscription; virtual private network [VPN] service)
- NoScript (free; Script blocker for Firefox)
- EFF Privacy Badger (free; online-tracking blocker for Chrome, Firefox, and Opera)

The Ultimate Utilities List, continued:

Drive diagnostics and management

- Paragon Drive Copy Pro (paid; migration and backup)
- EFD Software HD Tune (trial/paid; drive diagnostics)
- Paragon Partition Manager (free/paid; partitioning)
- EaseUS Partition Master (trial/paid; partitioning)
- EaseUS Todo Backup (free/paid; backup and restore)

Mobility

- Softpedia CoreTemp (free)

Password vaults

- AgileBits 1Password (trial/paid); top rating by Consumer Reports Online
- LastPass (free/paid)
- Siber Systems RoboForm (free/paid)

Online password checkers

- Gibson Research Corporation How big is your haystack? (free)
- How secure is my password? (free)
- Password Meter (free)

The Ultimate Utilities List, continued:

On-demand antivirus scanners

- Trend Micro HouseCall (free)
- Malwarebytes (free/paid)
- Windows Defender Offline (free; for Win7 and Win8.1, built into Windows 10)

Encryption

- Boxcryptor (free/paid; cloud-storage encryption)
- VeraCrypt (free/paid; the successor to TrueCrypt)

Firewall checkers

- ShieldsUP (Gibson Research Corporation; free)

Networking

- Metageek inSSIDer (sign-up required)
- Wireshark (free)

Addendum – Ask Woody Forum Topics

You can access these without a logon -

1) Setting up a Standard User Account in Windows 10 - protect your Admin. Account. (Thread started January 20, 2020)

https://www.askwoody.com/forums/topic/creating-a-standard-user-account-on-windows-10/?mc_cid=3c2c685596&mc_eid=c3d7529d95

2) Reader discussion of Backup Imaging Software:

https://www.askwoody.com/forums/topic/imaging-software-2/?mc_cid=0039c85858&mc_eid=c3d7529d95

(sorry, this link is apparently too long to convert to active; copy and paste it into a browser)

Macrium Reflect seems to come out on top over Terabyte, with Aeomi and Acronis also mentioned. Two users had negative experiences with Acronis. But,

If you happen to have a Western Digital hard drive or SSD in your computer, there's a free Western Digital Edition of Acronis available, but some limitations on its features.